Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования. "Астраханский Государственный Технический Университет"

Правовые основы информационной безопасности

ВЫПОЛНИЛ: СТУДЕНТ ГРУППЫ ДЮЮОБ-12/1

КАРИМОВ С.В.

ПРОВЕРИЛ: АССИСТЕНТ КАФЕДРЫ КОНСТИТУЦИОННОГО

И АДМИНИСТРАТИВНОГО ПРАВА ДАНИЛОВ В.А.

Основные документы РФ по ИБ

- Окинавская хартия информационного общества

- Доктрина информационной безопасности Российской федерации

Основные законы РФ по обеспечению ИБ

- Об информации, информатизации и защите информации.
- О связи.
- Об участии в международном информационном обмене.
- О государственной тайне
- О правовой охране программ для ЭВМ и баз данных.

Понятие «информационная безопасность»

- Информационная безопасность государства заключается в невозможности нанесения ущерба деятельности государства по выполнению функций в информационной сфере по управлению обществом и поддержанием порядка.

Государственная политика в области ИБ

- Федеральная программа ИБ
- Нормативно-правовая база
- Регламентация доступа к информации
- Юридическая ответственность за сохранность информации
- Контроль за разработкой и использованием средств защиты информации
- Предоставление гражданам доступа к мировым информационным системам

Информационная война

- Распространение ложной информации
- Манипулирование личностью.
- Разрушение традиционных духовных ценностей
- Навязывание инородных духовных ценностей
- Искажение исторической памяти народа
- Кибертерроризм

Национальные интересы в информационной сфере

- Обеспечение прав и свобод граждан на получение и распространение информации
- Обеспечение деятельности субъектов национальных интересов в информационной инфраструктуре общества (овладение надлежащей информацией и удовлетворение потребителей по ее использованию)

СМИ и ИБ

- Реализация потенциальной возможности манипулирования населением с помощью СМИ .
- Изменение акцентов в распространяемой информации.
- Распространение «правдоподобной» информации под видом истинной.
- Навязывание оценок событиям в интересах конкретных общественных групп.

Угрозы информационной безопасности

- 1. Уничтожение информационных объектов
- 2. Утечка информации
- 3. Искажение информации
- 4. Блокирование объекта информации

Объекты защиты информации

- Владельцы и пользователи
- Носители и средства обработки
- Системы связи и информатизации
- Объекты органов управления

Конфиденциальность информации

- Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней.

Целостность информации

- Существование информации в неискаженном виде, т.е. в неизменном по отношению к некоторому фиксированному ее состоянию.

Доступность информации

- Свойство системы, характеризующееся способностью обеспечивать своевременный и беспрепятственный доступ к информации субъектов соответствии с запросами

Аппаратно-программные средства ЗИ

- Системы идентификации и аутентификации пользователей
- Системы шифрования данных на дисках
- Системы шифрования данных, пересылаемых по сети
- Системы аутентификации электронных данных
- Средства управления ключами

Угрозы проникновения

- Маскарад-пользователь маскируется под другого пользователя.
- Обход защиты-использование слабых мест в системе безопасности с целью получения доступа.
- Нарушение полномочий-использование ресурсов не по назначению.
- Троянские программы-программы, содержащие программный код, при выполнении которого нарушается функционирование системы безопасности.

Противодействие техническим средствам разведки

- Формирование системы противодействия ТСР
- Скрытие демаскирующих признаков
- Противодействие распознаванию объекта
- Техническая дезинформация (подавление демаскирующих сигналов)
- Контроль эффективности противодействия ТСР

Способы реализации угроз информационной безопасности

- Непосредственное обращение к объектам доступа.
- Создание программных и технических средств с целью обхода средств защиты.
- Модификация средств защиты, позволяющая реализовать угрозы ИБ.
- Внедрение в ИС программных или технических средств, нарушающих функции ИС.

Угрозы раскрытия параметров системы

- Определение типа и параметров носителей информации
- Получение информации о программно-аппаратной среде, о функциях, выполняемых ИС, о системах защиты.
- Определение способа представления информации.
- Определение качественного содержания данных

Угроза нарушения конфиденциальности

- Хищение носителей информации.
- Несанкционированный доступ к ИС.
- Выполнение пользователем несанкционированных действий.
- Перехват данных, передаваемых по каналам связи.
- Раскрытие содержания информации.

Угроза отказа доступа

- Выведение из строя машинных носителей информации.
- Проявление ошибок разработки программного обеспечения.
- Обход механизмов защиты.
- Искажение соответствия конструкций языка.

Угроза нарушения целостности

- Уничтожение носителей информации
- Внесение несанкционированных изменений в программы и данные.
- Установка и использование нештатного программного обеспечения.
- Заражение вирусами
- Внедрение дезинформации

Средства обеспечения ИБ

- Правовые, политические. организационные средства.
- Технологические., кадровые, материальные, финансовые, информационные, научные средства.

Угрозы от персонала

- Разглашение
- Передача сведений о защите
- Халатность
- Вербовка
- Подкуп персонала
- Уход с рабочего места
- Физическое устранение

Исходные положения обеспечения ИБ

- ИБ основывается на требованиях законов, стандартов и нормативных документах.
- ИБ обеспечивается комплексом мер-организационных, программных, аппаратных.
- Средства защиты должны предусматривать контроль их эффективности.
- Средства защиты должны допускать оценку их эффективности.
- Средства защиты не должны снижать функциональные характеристики ИС.

Принципы обеспечения ИБ

- Системность
- Комплексность
- Непрерывность защиты
- Разумная достаточность
- Открытость алгоритмов защиты
- Простота применения защиты

Принцип системности

- Учет всех элементов, условий, факторов при всех видах информационной деятельности, при всех режимах функционирования, на всех этапах функционального цикла,при всех видах взаимодействия с внешней средой.

Принцип комплексности

- Согласование всех разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее элементов.

Принцип непрерывности

- Принятие соответствующих мер защиты на всех этапах жизненного цикла ИС от разработки до завершения этапа функционирования.

Разумная достаточность

- При достаточном времени и средствах преодолевается любая защита.Поэтому имеет смысл создавать только достаточный уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемы.

Гибкость системы защиты

- Средства защиты должны варьироваться применительно к изменяющимся внешним условиям и требованиям к уровню защищенности ИС.

Открытость механизмов защиты

- Знание алгоритмов защиты не должно давать средств и возможностей ее преодоления.Это не означает, что информация о системе защиты должна быть общедоступна-параметры системы должны быть также защищены.

Принцип простоты применения средств защиты

- Механизмы защиты должны быть понятны и просты в использовании.Не должны использоваться специальные языки, малопонятные или трудоемкие для пользователя дополнительные действия.

Уровни безопасности

- Базовый. Средства защиты должны противостоять отдельным атакам физических лиц.
- Средний. Средства защиты должны противостоять коллективным атакам лиц, обладающих ограниченными возможностями.
- Высокий. Средства защиты должны противостоять коллктивным атакам злоумышленника с потенциально неограниченными возможностями.

Причины утечки информации

- Несоблюдение персоналом норм, требований, правил эксплуатации ИС.
- Ошибки в проектировании ИС и систем защиты ИС.
- Ведение противостоящей стороной технической и агентурной разведки.

Виды утечки информации (гост Р 50922-96)

- Разглашение
- Несанкционированный доступ к информации
- Получение защищаемой информации разведками

Каналы утечки информации

- Электромагнитный канал(частотный , сетевой, линейный каналы и заземление)
- Акустический канал
- Визуальный канал
- Информационный канал(линии связи, локальные сети,машинные носители информации, терминальные и периферийные устройства)

Безопасная система

- Управляет доступом к информации так, что только авторизованные лица или процессы, действующие от их имени, получают право читать, писать и удалять информацию.

Надежная система по доступу

- Система, использующая достаточные аппаратные и программные средства для обеспечения одновременной обработки информации разной степени секретности группой пользователей без нарушения прав доступа.

Политика безопасности

- Совокупность правил и норм по уровню информационной безопасности, по характеру и способам обрабатываемой информации, правилам ее хранения и доступа и применяемым средствам защиты.

Основные механизмы безопасности

- Идентификация и аутентификация
- Управление доступом
- Протоколирование и аудит
- Криптография
- Экранирование
- Физическая защита инфраструктуры

Надежность системы по безопасности

- Соответствие сформулированной политике безопасности.
- Гарантированность-уровень доверия, которое может оказано конкретной реализации системы.

Этапы реализации механизмов ИБ-1

- 1) Формулировка угроз и выбор стандартов безопасности
- 2)Декомпозиция информационной системы
- 3) Анализ потов информации
- 4) Разработка (выбор) мер информационной защиты
- 5) Определение иерархии угроз по степени опасности.

Этапы реализации механизмов ИБ-2

- 6) Определение иерархии защитных мероприятий
- 7) Формулировка политики безопасности
- 8) Анализ вероятности угроз
- 9) Анализ человеческого фактора
- 10) Анализ опасности перехвата данных

Этапы реализации механизмов ИБ-3

- 11) Определение реакций на нарушения режима ИБ
- 12) Проверка сервисов безопасности на корректность
- 13) Реализация механизма идентификации и аутентификации
- 14) Выбор парольной системы
- 15) Реализация протоколирования и аудита

Этапы реализации механизмов ИБ-4

- 16) Выбор стандартов шифрования
- 17) Установка механизмов экранирования
- 18) Установка технических средств идентификации (электронные замки и т.п.)
- 19) Организация режима поддержки работоспособности системы
- 20) Определение направлений модернизации системы в случае обнаружения слабости информационной защиты

Стандарт защищенности США

- «Оранжевая книга»- стандарт США, принят в 1985 г. Предоставляет производителям и экспертам стандарт для разрабатываемых программных продуктов по обеспечению требований гарантированной защищенности при обработке информации.

Европейские критерии ИБ

- Стандарт ISO-IEC 15408. Общие критерии оценки информационной безопасности.
- Стандарт ISO 17799. Международный стандарт сетевой безопасности.
- Ripe MD-160. Стандарт цифровой подписи.

Российские стандарты ИБ

- Стандарт шифрования ГОСТ 28147-89
- Стандарт хэш-функции ГОСТ Р 34.11-94
- Стандарт цифровой подписи ГОСТ Р 34.10-94
- Средства вычислительной техники. Защита от НСД. Общие технические требования. ГОСТ Р 50739-95

Ресурсы Internet по ИБ

- www.sec.ru
- www.jetinfo.isib.ru
- www.sbcinfo.ru
- www.cryptography.ru
- www.agentura.ru
- www.infosecurity.ru